THE CANADIAN BAR REVIEW

LA REVUE DU BARREAU CANADIEN

Vol. 103 2025 No. 2

"TURNING BREADCRUMBS INTO DIALOGUE: AN INSTITUTIONAL JUSTIFICATION FOR *R V BYKOVETS*"

Colton Fehr[1]

The Supreme Court of Canada concluded in R v Spencer that individuals maintain a reasonable expectation of privacy in their internet service provider (ISP) subscriber information. Ten years later, the Court in R v Bykovets built upon this ratio by concluding that state access to an accused's internet protocol (IP) address—a step preceding any application to produce ISP subscriber information—also attracts a reasonable expectation of privacy. While ISP subscriber information necessarily reveals online activity, the majority held that an IP address itself attracts a reasonable expectation of privacy despite private information only being revealable if further investigative steps were taken. A narrow dissent concluded that the reasonable expectation of privacy inquiry should take its hue from the ability of the precise information sought to reveal inherently private information. As IP addresses themselves only reveal the name of the issuing ISP, no reasonable expectation of privacy could arise from obtaining an IP address from a third party. Given the force of this objection, it is prudent to consider whether a different justification—based on the appropriate relationship between courts and legislatures when crafting criminal procedure rules—can provide an alternative defence of the majority's conclusion. While institutional considerations bolster the majority's decision, I also maintain that Parliament should respond to Bykovets and Spencer with narrowly tailored laws permitting limited access to IP addresses and ISP subscriber information on administrative demand.

[1] Assistant Professor, University of Saskatchewan, College of Law. I wish to thank Robert Diab and the anonymous reviewers for their thoughtful comments on this article.

La Cour suprême du Canada a conclu, dans l'arrêt R c Spencer, que les gens ont une attente raisonnable en matière de respect de la vie privée par rapport aux renseignements d'abonnés détenus par les fournisseurs d'accès Internet (FAI). Dix ans plus tard, elle a renchéri dans l'arrêt R c Bykovets, statuant que l'accès de l'État à l'adresse IP d'un accusé—étape préalable au dépôt d'une demande de renseignements d'abonnés auprès d'un FAI—s'accompagne aussi de cette attente. Même si les renseignements d'abonnés donnent forcément des indications sur les activités en ligne, la majorité des juges a soutenu que l'adresse IP elle-même est aussi visée par une attente raisonnable en matière de respect de la vie privée, malgré le fait que des renseignements de nature privée ne sont divulgués que si d'autres mesures d'enquête sont prises. Une minorité dissidente a quant à elle conclu que ce type d'attente devrait reposer sur la possibilité que des données précises recherchées révèlent, par essence, des renseignements de nature privée. Comme les adresses IP ne révèlent que le nom du FAI à leur origine, leur obtention auprès d'un tiers ne devrait être assortie d'aucune attente raisonnable en matière de respect de la vie privée. Vu la force de cette objection, il faut se demander s'il est possible de justifier autrement la conclusion de la majorité, selon la relation souhaitable entre les tribunaux et les assemblées législatives chargés de rédiger les règles de procédure en matière criminelle. Même si les facteurs institutionnels sous-tendent la conclusion de la majorité, l'auteur soutien que le Parlement devrait réagir aux arrêts Bykovets et Spencer en adoptant des lois visant expressément à limiter l'accès aux adresses IP et aux renseignements d'abonnés des FAI en cas de requête administrative.

Contents

Introduction

In *R v Bykovets*,[2] the Supreme Court of Canada was asked whether individuals maintain a reasonable expectation of privacy in their Internet Protocol (IP) addresses within the meaning of section 8 of the *Canadian Charter of Rights and Freedoms*.[3] The Court's resolution of this issue built upon its prior decision in *R v Spencer*,[4] wherein the Court found that an individual maintains a reasonable expectation of privacy in their Internet Service Provider (ISP) subscriber information.[5] Accessing ISP subscriber information will nevertheless typically tell authorities precisely who used an already known IP address at a particular time and place.[6] In contrast, knowledge of an IP address can only reveal the user's identity if combined with other information.[7] Despite the IP address not being used in this manner in *Bykovets*, the majority found that the offender maintained a reasonable expectation of privacy. As Justice Karakatsanis explained, "an IP address is the first digital breadcrumb that can lead the state on the trail of an individual's Internet activity" and therefore "may betray personal information long before a *Spencer* warrant is sought."[8]

Writing for a four-judge dissent, Justice Côté contended that any reasonable expectation of privacy claim was rendered moot by the fact that the police refrained from using the IP address to reveal personal information about the offender. The officers instead proceeded appropriately when they employed the only procedure left open to them after *Spencer* to compel the ISP to release the subscriber information relating to the IP address: obtaining a production order under section 487.014 of the *Criminal Code of Canada*.[9] In criticizing the majority judgment, the minority asserted that finding a reasonable expectation of privacy existed in the circumstances would "seriously thwart the police's ability to investigate … serious offences."[10] Citing Justice Moldaver's reasons in *R v Marakah*,[11] Justice Côté agreed that increasing the hurdles for obtaining "these judicial authorizations could strain police and judicial resources in an

---

2 2024 SCC 6 [*Bykovets*].

3 Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c11 [*Charter*].

4 2014 SCC 43 [*Spencer*].

5 *Ibid* at para 66.

6 I say "typically" as cases wherein many individuals use the same computer could give rise to doubt about who is the guilty party.

7 See *Bykovets*, *supra* note 2 at paras 60–70 (reasons of Justice Karakatsanis), 132–35 (reasons of Justice Côté).

8 *Ibid* at para 9.

9 RSC 1985, c C-46 [*Criminal Code*].

10 See *Bykovets*, *supra* note 2 at para 160.

11 2017 SCC 59 [*Marakah*].

already overburdened criminal justice system. Investigations would be slowed, more judicial officers would be required, and the administration of criminal justice as a whole will suffer."[12]

While I find the dissenting view persuasive, I nevertheless contend that the result in *Bykovets* can be defended on institutional grounds. Longstanding debates about the appropriate role of courts and legislatures when crafting criminal procedure rules—and digital privacy rules in particular—suggest that courts are better equipped to identify privacy concerns given their counter-majoritarian role. However, courts have proven less capable of devising principled rules to govern such searches given the complex factual matrices and rapidly shifting nature of privacy interests, especially in the digital age.[13] These concerns should be read alongside the majority's salient observation that failure to recognize a reasonable expectation of privacy in *Bykovets* can reasonably be thought to jeopardize privacy interests due to difficulties in uncovering breaches engaging digital privacy interests in particular.[14] Protection of these interests can accordingly be promoted by courts considering privacy violations that *could* arise given reasonably foreseeable uses of technology. This in turn should have the salutary effect of motivating Parliament to do a job that it has become increasingly reluctant to do: craft criminal procedure rules.[15]

If I am correct that the majority's reasons are defendable on institutional grounds, a single means exists to address the legitimate law enforcement concerns raised by the Crown: legislative intervention. By enacting a law that allows police to compel IP addresses (and ISP subscriber information),[16] Parliament can set the parameters of the debate about the proper balance between privacy and law enforcement interests in a way that the *Bykovets* Court could not. In particular, Parliament

---

12 See *Bykovets*, *supra* note 2 at para 160, citing *Marakah*, *supra* note 11 at para 185.

13 For my prior work on this point, see Colton Fehr, "Digital Evidence and the Adversarial System: A Recipe for Disaster?" (2018) 16:2 CJLT 437; Colton Fehr, "Criminal Law and Digital Technologies: An Institutional Approach to Rule Creation in a Rapidly Advancing and Complex Setting" (2019) 65:1 McGill LJ 67; Colton Fehr, "Criminal Law & Digital Technologies: Drawing Lessons from the Canadian and American Experiences" (2021) 53:3 UBC L Rev 653.

14 See *Bykovets*, *supra* note 2 at paras 53–55.

15 For perhaps the most influential (albeit early) account, see James Stribopoulos, "In Search of Dialogue: The Supreme Court, Police Powers, and the *Charter*" (2005) 31:1 Queen's LJ 1. For my review of the relevant legislation in the digital privacy context, see the articles cited *supra* note 13.

16 See Colton Fehr, "A Proposal for Police Acquisition of ISP Subscriber Information on Administrative Demand in Child Pornography Investigations" (2019) 24:2 Can Crim L Rev 235.

can state that this information can be compelled with respect to certain criminal investigations so long as additional procedural safeguards are respected. Such an approach is institutionally prudent as it encourages dialogue between the respective branches and allows each to ascribe full weight to the interests engaged by section 8 of the *Charter* that they are best equipped to protect. This is not to say that courts ought to show deference when answering the question of whether any balance struck by Parliament between privacy and law enforcement interests is reasonable. With a law passed through legislative process, the courts will simply be better placed to make such a determination as they will have the benefit of legislative study and debate to develop a fuller understanding of the relevant state interests.

The article unfolds as follows. In Part I, I review the Supreme Court's decision in *Bykovets* and problematize the majority's rationale for finding that state access to an IP address intrudes upon a reasonable expectation of privacy. In Part II, I then contend that the majority's conclusion can nevertheless be defended on institutional grounds. Permitting courts to rely upon hypothetical scenarios when determining whether a reasonable expectation of privacy exists vis-à-vis a search tactic ensures that privacy interests are more likely to be litigated. At the same time, such an approach encourages Parliament to respond with a more robust set of police powers to ensure effective law enforcement. The courts can thereafter test those reply laws for consistency with section 8 of the *Charter* under its "reasonableness" prong. I conclude in Part III by reviewing the legislative context within which police must operate when seeking IP addresses and ISP subscriber information necessary to forward a host of online criminal investigations. I contend that the current legislation can be supplemented with considerably more permissive police powers that do not require prior judicial authorization. Instead, privacy may be protected in other ways such as by restricting the investigations for which such administrative demands may be made and statutorily compelling exclusion of evidence if police abuse their proposed power.

I. Privacy Interests in IP Addresses

The accused in *Bykovets* was convicted at trial of 14 property offences resulting from the fraudulent use of credit card data to purchase various items.[17] The police learned during its investigation that one of the stores from which fraudulent purchases were made was managed by a company called Moneris, a third-party payment processing company. The police subsequently contacted Moneris and requested that it voluntarily disclose

---

17 See *Bykovets*, *supra* note 2 at para 15.

the IP addresses behind the relevant purchases.[18] After receiving this information, the police used a publicly available database to identify the ISP that issued the IP address.[19] With this information in hand, the police were able to obtain a production order compelling Telus to disclose the ISP subscriber information behind the IP addresses.[20] The police then used the knowledge that the appellant and his father were behind the fraudulent transactions as evidence to support the issuance of a search warrant for the offenders' residences wherein various pieces of incriminating evidence were located.[21]

The main issue raised at trial was whether the accused possessed a reasonable expectation of privacy within his IP address.[22] If so, then the state request for the IP address from the third-party company would constitute a "search" as that term is defined under section 8 of the *Charter*. As the police obtained no prior authorization to request the IP address, the search would necessarily fail the first requirement for a search to be "reasonable," namely, it must be "authorized by law."[23] The search would accordingly run afoul of the protection against "unreasonable search or seizure" provided under section 8 of the *Charter*. As both the trial court and majority of the Court of Appeal of Alberta answered this question in the negative, neither court definitively answered whether a potential section 8 *Charter* violation warranted any remedy when considered alongside other breaches of the accused's rights pertaining to sections 7 and 10(b) of the *Charter*.[24]

A narrow majority of the Supreme Court overturned both lower courts on the question of whether a breach of section 8 of the *Charter* occurred when the police asked Moneris to disclose the relevant IP address. In so doing, the Court applied what is now a long-settled legal framework for determining whether an accused maintains a reasonable expectation of privacy with respect to a state investigative technique. Four avenues of inquiry are relevant to answering this question. First, it is necessary to define the subject matter of the search. Second, courts must determine whether the claimant maintains an interest in the subject matter. Third, the

---

18 *Ibid* at para 16.

19 *Ibid* at para 98.

20 *Ibid* at para 16.

21 *Ibid* at para 17.

22 *Ibid* at para 28.

23 See *R v Collins*, [1987] 1 SCR 265 at 278.

24 See *R v Bykovets*, 2020 ABQB 70 at para 84 (requiring submissions on remedy pertaining to section 7 and 10(b) breaches only); *R v Bykovets*, 2022 ABCA 208 at paras 31–37 (reasons of majority finding that other *Charter* violations did not warrant exclusion but also holding that no section 8 breach occurred), and 98 (finding a section 8 breach and returning the issue of remedy to the trial judge to consider alongside the other breaches).

accused must demonstrate that they maintained a subjective expectation of privacy and, finally, that their expectation of privacy is objectively reasonable in the circumstances.[25]

The diverging opinions in *Bykovets* centred upon the first avenue of inquiry—the subject matter of the search—and how the subject matter's framing impacted the final assessment of whether the expectation of privacy was objectively reasonable. The justices agreed that the subject matter must be determined by considering the question: "what were the police really after?"[26] The accused maintained that the state sought "to connect an internet activity to a specific person" and submitted that "[o]btaining an IP address was an essential step in identifying the internet user responsible for specific internet activity."[27] In contrast, the Crown contended that the police "wanted the IP addresses for a much simpler purpose: "to further [their] investigation."[28] In rejecting the latter position, the majority took a "holistic view of the subject matter" that was not "mechanical" and reflected "technological reality."[29] This view was arguably supported by numerous of the Court's precedents. In *R v Reeves*,[30] for instance, the Court held that the state's seizure of a computer gave rise to a reasonable expectation of privacy in large part because the police "obtained the means through which to access [highly private] information" even though the state required a subsequent warrant to search the computer.[31] Applying this rationale in *Bykovets*, the majority observed that an IP address similarly "provided the state with the means through which to draw immediate and direct inferences about the user behind specific Internet activity."[32]

In determining whether the search of the IP address was objectively reasonable, the majority observed that the issue turns on three factors: "the claimant's control over the subject matter, the place of the search, and the private nature of the subject matter."[33] The place of the search is

---

25 See *Spencer*, *supra* note 4 at para 18, citing *R v Tessling*, 2004 SCC 67 at para 32 [*Tessling*].

26 See *Bykovets*, *supra* note 2 at paras 34, 123, citing *Marakah*, *supra* note 11 at para 15.

27 See *Bykovets*, *supra* note 2 at para 35.

28 *Ibid* at para 36.

29 *Ibid* at para 34, citing *Spencer*, *supra* note 4 at paras 26, 31; *Marakah*, *supra* note 11 at para 17.

30 2018 SCC 56 [*Reeves*].

31 See *Bykovets*, *supra* note 2 at para 40, citing *Reeves*, *supra* note 30 at para 34.

32 See *Bykovets*, *supra* note 2 at para 41. See also para 136 (dissenting reasons of Justice Côté).

33 *Ibid* at para 45, citing *Marakah*, *supra* note 11 at para 24. While other factors will be relevant in different contexts, these three factors were the only ones discussed in

of limited relevance in the digital context given the qualitatively different nature of online and physical spaces.[34] Similarly, absence of control over informational data is not determinative of a privacy claim.[35] Relying on *R v Jones*,[36] Justice Karakatsanis agreed that individuals "may choose to divulge certain information for a limited purpose, or to a limited class of persons, and nonetheless retain a reasonable expectation of privacy."[37] Given the importance of anonymity to fostering expression on the internet,[38] such a choice must be viewed in the relevant social and economic context within which it is made. Citing *Jones*, Justice Karakatsanis affirmed that retaining control is impossible in light of the stark choice it presents individuals: give up control of one's data or make no use of internet services.[39] As she rightly concludes, "Canadians are not required to become digital recluses in order to maintain some semblance of privacy in their lives."[40]

In light of the limited utility of the other two factors, whether a reasonable expectation of privacy existed turned most directly upon the private nature of the subject matter. Such an inquiry necessarily begins with acknowledging that section 8 of the *Charter* seeks "to protect a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state" and thus "include[s] information which tends to reveal intimate details of the lifestyle and personal choices of the individual."[41] Recognition of a privacy claim is therefore meant to extend as far as needed "to protect individual dignity, autonomy, and personal growth, and no further."[42] In the majority's view, these interests are best served by factoring into the analysis information that *could* be revealed as a result of obtaining an IP address. While police did not use the IP address in *Bykovets* in an improper manner, all parties agreed with an expert witness who cogently explained how internet activity could be revealed with nothing more than

---

Bykovets.

34 See *Bykovets*, *supra* note 2 at para 49, citing *R v Ramelson*, 2022 SCC 44 at para 49.

35 See *Bykovets*, *supra* note 2 at para 46, citing *Reeves*, *supra* note 30 at para 38.

36 2017 SCC 60 [*Jones*].

37 *Ibid* at para 39.

38 See *Spencer*, *supra* note 4 at para 45, citing Alan Westin, *Privacy and Freedom* (New York: Athenium, 1967) ("[o]ne form of anonymity … is what is claimed by an individual who wants to present ideas publicly but does not want to be identified as their author" at 32).

39 See *Bykovets*, *supra* note 2 at para 48, citing *Jones*, *supra* note 36 at para 45.

40 See *Bykovets*, *supra* note 2 at para 48.

41 *Ibid* at para 51, citing *R v Plant*, [1993] 3 SCR 281 at 293.

42 See *Bykovets*, *supra* note 2 at para 52.

an IP address when the digits forming the address are combined with other information the state could easily acquire.[43]

The majority in *Bykovets* defended its reliance upon information that could be revealed after retrieving an IP address to establish a reasonable expectation of privacy on normative grounds. As Justice Karakatsanis observed, whether a reasonable expectation of privacy existed cannot be determined "according to only one particular use of the evidence. Nor can its reach be determined according to the police's specific intention in seeking the information."[44] Instead, she insisted that "the purpose of s. 8, appreciated normatively, requires that we ask what information the subject matter of the search tends to reveal. Because this analysis seeks to determine 'whether people generally have a privacy interest' in the subject matter of the state's search, we consider not only the information that police seek to uncover in a particular case, but all the information that the subject matter may tend to uncover."[45] This interpretation of section 8 of the *Charter* was cited to the Supreme Court's reasons in *R v Patrick*.[46] As the majority opined in that case, the reasonable expectation of privacy analysis is "laden with value judgments which are made from the independent perspective of the reasonable and informed person who is concerned about the long-term consequences of government action for the protection of privacy."[47]

Writing for a four-judge dissent, Justice Côté disagreed with the majority's framing of the subject matter of the search. Applying the same analytical framework, she maintained that courts ought not be concerned with the investigating officer's objective in the particular criminal investigation or their subjective intentions in conducting the search.[48] Instead, courts are "concerned with the capacity of the precise information sought to give rise to inferences or to reveal *further* information."[49] Justice Côté used the Supreme Court's decision in *Spencer* to illustrate this narrower approach. As she explained, the contention that the plain ISP subscriber information was the subject matter of the search was rightly rejected in *Spencer*. Such a characterization, the *Spencer* Court concluded, "gloss[es] over the significance of an IP address and what such an address, *once identified with*

---

43 *Ibid* at paras 60–70. As the conclusion that details of internet activity can be revealed with a bare IP address when combined with other third-party website information is uncontested, it is unnecessary to provide a detailed review of the search method.

44 *Ibid* at para 53, citing *R v Patrick*, 2009 SCC 17 at para 32 [*Patrick*].

45 See *Bykovets*, *supra* note 2 at para 53, citing *Patrick*, *supra* note 44 at para 32.

46 *Patrick*, *supra* note 44.

47 *Ibid* at para 14.

48 See *Bykovets*, *supra* note 2 at para 123.

49 *Ibid*.

a particular individual, is capable of revealing about that individual."[50] The Court in *Spencer* accordingly "concluded that the subject matter of the search was 'the identity of a subscriber whose Internet connection is linked to particular, monitored Internet activity.'"[51] It was thus vital in *Spencer* that "[t]he precise information sought—subscriber information—provided a link between a specific individual and the particular online activity associated with an anonymous IP address. All of this constituted the subject matter of the search."[52]

The dissent in *Bykovets* also drew on other Supreme Court jurisprudence applying the reasonable expectation of privacy test to bolster its conclusion.[53] In *R v Marakah*,[54] for instance, the accused sent text messages containing criminal content to his accomplice. As the messages from the accused's phone were improperly obtained, the prosecution attempted to admit the messages from the accomplice's phone to establish his participation in the charged offences. In concluding that the accused maintained a reasonable expectation of privacy in the latter messages, the Court in *Marakah* did not find that the subject matter of the search was the cell phone seized by police.[55] As Justice Côté observed, the subject matter of the search "included text message conversations contained in the cell phone as well as any inferences about associations and activities 'that can be drawn *from th[e] information*' shared in those conversations."[56] It followed that the subject matter was framed in such a way that "the capacity of the precise information sought to give rise to inferences or to reveal further information must be supported by the evidence; it cannot be based on mere conjectures or hypotheses."[57]

In arriving at this conclusion, Justice Côté was cognizant of the fact that her disagreement with the majority judges turned on the impact finding a reasonable expectation of privacy in an IP address would have on law enforcement interests. In her view, the majority's approach threatened to "upset the careful balance that this Court has struck between the interest of Canadians in actual privacy and the interest of Canadians in not hindering

---

50 *Ibid* at para 124, citing *Spencer*, *supra* note 4 at para 32; *R v Trapp*, 2011 SKCA 143 at para 35 [emphasis added in *Bykovets*].

51 See *Bykovets*, *supra* note 2 at para 124, citing *Spencer*, *supra* note 4 at para 33.

52 See *Bykovets*, *supra* note 2 at para 124.

53 *Ibid* at paras 126–28, citing *R v Kang-Brown*, 2008 SCC 18 [*Kang-Brown*]; *R v Gomboc*, 2010 SCC 55.

54 *Supra* note 11.

55 See *Bykovets*, *supra* note 2 at para 125.

56 *Ibid*, citing *Marakah*, *supra* note 11 at para 20 [emphasis added in *Bykovets*].

57 See *Bykovets*, *supra* note 2 at para 126.

law enforcement."[58] As I explain in more detail below, this balance is impacted because finite resources must now be inefficiently deployed which in turn will limit the state's capacity to fight crime.[59] This argument has particular force in light of the fact that judicial approval is currently necessary before any tactic—including the tactic raised by the majority of combining IP addresses with third-party website information[60]—can be employed by state actors to reveal online activity.[61] Justice Karakatsanis nevertheless notes that a request for an IP address will often be rolled into an ISP subscriber information application. She therefore asserts that the majority's decision does "not unduly interfere with law enforcement's ability to deal with … crime."[62] Justice Karakatsanis is no doubt correct that the impact of the majority's decision can be mitigated by combining applications. In my view, however, it is not intuitive that even a minimal interference with law enforcement interests should be tolerated when the privacy interest relied upon are based on "mere conjectures or hypotheses."[63]

II. An Institutional Justification for *Bykovets*

The majority in *Bykovets* frequently appealed to the purpose of section 8 of the *Charter* in defending its expansive deployment of that provision.[64] As Justice Karakatsanis observes, the purpose of section 8 is to *prevent* unreasonable searches and seizures.[65] An approach that draws attention to potential state action that is capable (even if not done in the instance

---

58 *Ibid* at para 139, citing *Tessling*, *supra* note 25 at para 17; *Kang-Brown*, *supra* note 53 at para 10; *R v Vu*, 2013 SCC 60 at para 21; *R v Stairs*, 2022 SCC 11. See also paras 160–64.

59 See *Bykovets*, *supra* note 2 at para 160, citing *Marakah*, *supra* note 11 at para 185 (reasons of Justice Moldaver).

60 For a more detailed description of how an IP address can be used to reveal online activity, see Justice Karakatsanis' explanation in *Bykovets*, *supra* note 2 at paras 60–70.

61 *Ibid* at para 135.

> Whether the identity of an anonymous Internet user is revealed by combining his or her IP address with subscriber information held by an ISP or by combining his or her IP address with other information held by thirdparty websites, the result is the same. The user's privacy interest in anonymity is undermined. Accordingly, as the Crown accepts, *Spencer* requires the police to obtain judicial authorization before requesting data of this nature—in other words, data that unveils the identity of an individual whose Internet connection is linked to particular, monitored online activity.

62 *Ibid* at para 85.

63 *Ibid* at para 126.

64 *Ibid* at paras 6, 13, 88, citing *Hunter v Southam Inc*, [1984] 2 SCR 145 [*Hunter*].

65 See *Bykovets*, *supra* note 2 at paras 6, 13, 88, citing *Hunter*, *supra* note 64.

case) of leading to significant privacy intrusions certainly is better able to prevent breaches of privacy than an approach that waits for a case to come along that directly raises the relevant privacy concern. If the dissent's approach in *Bykovets* were endorsed, the courts would remain silent until the state was caught using an IP address in a manner that revealed private information. Given the ability of a state actor to use digital data discreetly, and the profound implications for privacy implicated by such action,[66] the dissent's approach would allow for unknown privacy invasions until the point that a state action is litigated in the courts. As anyone with a passing understanding of the Canadian legal system knows, such a process may take many years and will cost the defendant an inordinate sum. While not made explicit, I suspect this reality was top of mind for the majority justices.

The majority's appeal to the purpose of section 8 of the *Charter* as a justification for relying upon a reasonable hypothetical scenario strikes me as a promising but incomplete argument for recognizing a reasonable expectation of privacy in an IP address. It is promising because courts should play a robust role in preventing intrusions onto privacy interests given the social realities of the criminal justice system. Such an argument is incomplete, however, because it inadequately explains why courts are better capable of identifying constitutional interests and ignores the appropriate role of legislatures in crafting criminal procedure rules. To the former question, it is commonly understood that courts applying a bill of rights serve a counter-majoritarian function. This follows because "courts are more independent and therefore less susceptible to special interest influence or majoritarian dislike of criminal suspects, who are disproportionately members of disadvantaged minorities."[67] Where infringements of privacy by the state are possible but difficult for litigants to uncover, crafting a constitutional rule to deter such breaches strikes me as prudent as it allows courts to more effectively fulfill their counter-majoritarian role.

---

66 See *Bykovets*, *supra* note 2 at para 69, citing *Jones*, *supra* note 36 at para 42; *R v Morelli*, 2010 SCC 8 at para 3; Susan Magotiaux, "Out of Sync: Section 8 and Technological Advancement in Supreme Court Jurisprudence" (2015) 71 SCLR (2d) 501 at 502.

67 See Fehr, "Digital Evidence", *supra* note 13 at 441, citing Lawrence Lessig, *Code: Version 2.0* (New York: Basic Books, 2006) at 216–22; David Sklansky, "Two More Ways Not to Think About Privacy and the Fourth Amendment" (2015) 82:1 U Chicago L Rev 223 at 227; Erin Murphy, "The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment, and Statutory Law Enforcement Exemptions" (2013) 111 Mich L Rev 485 at 535–36; Steven Penney, "Reasonable Expectations of Privacy and Novel Search Technologies: An Economic Approach" (2007) 97 J Crim L & Criminology 477 at 505–06; Kent Roach, *Due Process and Victims' Rights: The New Law and Politics of Criminal Justice* (Toronto: University of Toronto Press, 1999).

The *Bykovets* case is illustrative of the type of challenges that arise with proving a breach of many criminal procedure rules, and especially those implicating digital technologies. As numerous scholars observe, the costs of hiring a lawyer are financially prohibitive for many accused persons and therefore provide a significant barrier to *Charter* litigation.[68] Calling an expert witness—which will often be necessary in digital privacy cases given the complexity of digital technologies—can make the total cost debilitating for the vast majority of Canadians, let alone the typically impecunious criminal defendant. While the accused in *Bykovets* was able to call the required evidence, it is highly unlikely that many accused will be able to do so. Socio-economic realities may therefore result in questionable police investigative practices being deployed for lengthy periods of time without meaningful consideration of their constitutionality.

The Supreme Court recently accepted a similar argument in the context of using "reasonable hypothetical scenarios"—defined as scenarios that are not "marginally imaginable" or "far-fetched"[69]—as a means to challenge mandatory minimum sentences. Obviously, use of the prohibition against "cruel and unusual treatment or punishment" found in section 12 of the *Charter* to challenge mandatory minimum sentences provides a distinguishable context as the alleged unconstitutional state conduct arises during the legislative process. The animating principle underlying this jurisprudence is nevertheless instructive in the criminal procedure context as well. Citing Chief Justice McLachlin's reasons in *R v Nur*,[70] Justice Martin recently reiterated in *R v Hills*[71] that "[i]f the only way to challenge an unconstitutional law were on the basis of the precise facts before the court, bad laws might remain on the books indefinitely."[72] Similarly, if the only way to challenge a search or seizure tactic were on the basis of the precise facts before the court, "bad investigative practices" that are difficult for litigants to challenge may persist.

---

[68] See e.g. Benjamin Berger, "Putting a Price on Dignity: The Problem of Costs in *Charter* Litigation" (2002) 26:3 Advocates' Quarterly 235; Kent Roach, "Enforcement of the *Charter*—Subsections 24(1) and 52(1)" (2013) 62 SCLR (2d) 473 at 486; Robert Sharpe, "Access to *Charter* Justice" (2013) 63 SCLR (2d) 3 at 3; Andrew Petter, *The Politics of the Charter: The Illusive Promise of Constitutional Rights* (Toronto: University of Toronto Press, 2010) at 104–05; Larissa Kloegman, "A Democratic Defence of the Court Challenges Program" (2007) 16:3 Constitutional Forum 107 at 107; Joseph Arvay & Alison Latimer, "Cost Strategies for Litigants: The Significance of *R. v. Caron*" (2011) 54 SCLR (2d) 427 at 427, 448–49.

[69] See e.g. *R v Goltz*, [1991] 3 SCR 485 at 506, 515; *R v Morrisey*, 2000 SCC 39 at para 30; *R v Nur*, 2015 SCC 15 at para 56 [*Nur*].

[70] *Supra* note 69.

[71] 2023 SCC 2 [*Hills*].

[72] *Ibid* at para 72, citing *Nur*, *supra* note 69 at para 51.

Encouraging judges to identify a reasonable expectation of privacy based on a hypothetical scenario nevertheless ought not be taken as an endorsement of judicial rulemaking in the digital privacy context. I elsewhere explain in detail why many of the problems Orin Kerr[73] found in the American context with such judicial rule creation also arise in Canada.[74] Other Canadian scholars similarly find that legal actors tend to struggle understanding digital technologies and fitting them within traditional legal frameworks. Lawyers are therefore likely to leave evidentiary gaps and judges—especially (but not exclusively) when evidence is lacking—often craft ill-informed rules.[75] These legitimate concerns are nevertheless less worrisome when the sole issue is whether a reasonable expectation of privacy exists vis-à-vis a particular search tactic. This follows because such a finding does not compel a particular type of rule be crafted by courts or (more often) passed by Parliament. Determining whether an appropriate balance has been struck by any "authorized law" will instead turn on whether the relevant law enforcement and privacy interests are "reasonable" within the meaning of section 8 of the *Charter*.

By pointing to a hypothetical privacy infringement, courts therefore serve another salient function: encouraging Parliament to fill gaps in criminal procedure rules. Calls for greater legislative action with respect to criminal procedure rulemaking in Canada are longstanding and forceful.[76] From an institutional perspective, prominent scholars and judges contend that Parliament is better suited to craft criminal procedure rules because it is better capable of studying the relevant law enforcement and privacy interests and the myriad ways in which these interests may be balanced and invasions onto privacy mitigated.[77] I discuss this point at length in prior writing, pointing out how digital evidence especially is a "recipe

---

73 See generally Orin Kerr, "The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution" (2004) 102:5 Mich L Rev 801. See also Stephen Breyer, "Our Democratic Constitution" (2002) 77 NYUL Rev 245 at 261.

74 See e.g. Fehr, "Institutional Approach", *supra* note 13; Fehr, "Drawing Lessons", *supra* note 13.

75 See e.g. Daniel Scanlan, "Issues in Digital Evidence and Privacy: Enhanced Expectations of Privacy and Appellate Lag Times" (2012) 16:3 Can Crim L Rev 301 at 302; Steven Penney, "The Digitization of Section 8 of the *Charter*: Reform or Revolution?" (2014) 67 SCLR (2d) 505 at 530; Graham Mayeda, "My Neighbour's Kid Just Bought a Drone … New Paradigms for Privacy Law in Canada" (2016) 35:1 NJCL 59 at 79–81; Jordan Fine, "Leaving Dumb Phones Behind: A Commentary on the Warrantless Searches of Smartphone Data Granted in *R. v. Fearon*" (2015) 13:2 CJLT 171 at 177–81.

76 See e.g. Steve Coughlan, "Canada Needs a Code of Police Powers" (2022) 79 CR (7th) 55; Stribopolous, *supra* note 15.

77 Coughlan, *supra* note 76; Stribopolous, *supra* note 15. See also Penney, "Reasonable Expectations", *supra* note 67 at 501–05; *Dedman v R*, [1985] 2 SCR 2 (dissenting reasons of Chief Justice Dickson).

for disaster" when courts employ it to craft rules in the context of the adversarial system.[78] While majoritarian concerns make it prudent for courts to make determinations about whether a reasonable expectation of privacy exists, how the relevant interests are understood and balanced are arguably better determined through the legislative process.[79] An approach to constitutional rulemaking that encouraged Parliament to legislate more effectively with respect to criminal procedure rules—and especially those implicating the rapidly advancing field of search and seizure law—is therefore prudent from an institutional perspective.

To be clear, I do not wish to be understood as saying that courts should show any enhanced deference to how Parliament strikes a balance between relevant privacy and law enforcement concerns. Section 8 of the *Charter* simply requires that balance be "reasonable," a standard that courts have become adept at applying over 40 years of *Charter* jurisprudence. When provided with the legislative record explaining why a particular balance was struck between privacy and law enforcement interests, courts will be especially well-suited for this task as they will be better informed with respect to the relevant interests and therefore capable of determining whether that balance is reasonable. Courts will accordingly engage in dialogue with Parliament over the appropriate balance between privacy and law enforcement interests without having to bear the heavy burden of crafting the relevant criminal procedure rules, a task which it has not proven particularly adept.[80] If this approach is prudent, then I suggest that the majority in *Bykovets* could have relied upon these institutional considerations to justify its reliance upon a hypothetical scenario in finding a breach of section 8 of the *Charter*.

III. Crafting a Legislative Response

If my alternative defence of the majority's decision in *Bykovets* is persuasive, the question inevitably arises: how should Parliament respond to the Supreme Court's jurisprudence in light of the legitimate law enforcement concerns raised by internet crime? Parliament has yet to provide a significant response to *Spencer* or *Bykovets*. Instead, police are left to apply for orders to receive both an IP address and/or obtain subscriber information from an ISP. As I contend below, the importance of certain investigations and the challenges they present to law enforcement could render what I call an "administrative demand" law that effectively does

---

78 See generally Fehr, "Digital Evidence", *supra* note 13 (assessing the judicial experience using the common law to craft rules relating to cell phone searches incident to arrest).

79 *Ibid*.

80 I have developed this point at length in a series of articles *supra* note 13.

away with a judicial warrant requirement "reasonable" under section 8 of the *Charter* if certain privacy protections are put in place.

A) Existing Legislation

Two provisions of the *Criminal Code* are germane to investigations involving disclosure of IP addresses or ISP subscriber information to facilitate the investigation of crime. The first, as identified by the majority in *Bykovets*, is section 487.015.[81] This provision allows the police to make an *ex parte* application to a court for an order that a person "prepare and produce a document containing transmission data that is … in their possession or control" and is necessary to identify "a device or person involved in the transmission of a communication."[82] The issuing judge may make the order if, among other requirements, there are "reasonable grounds to suspect" that an individual behind the relevant communication—which includes an IP address—committed a crime.[83] To meet this standard, the applicant need only demonstrate that there is a "reasonable possibility" that the individual behind the relevant communication committed a crime.[84] If this standard is met, an order compelling the disclosure of an IP address will issue.

If the police know the relevant IP address—either due to an order under section 487.015 or because the IP address was inadvertently disclosed by the accused during the course of an investigation[85]—then police can apply for a production order under section 487.014 of the *Criminal Code*. This application allows police to receive the subscriber information belonging to the IP address when the crime was committed. In particular, section 487.014 states that "a justice or judge may order a person to produce a document that is a copy of a document that is in their possession or control when they receive the order, or to prepare and produce a document containing data that is in their possession or control at that time."[86] The issuing judge may make the production order if, among other requirements, the Crown demonstrates that there are "reasonable grounds to believe" that the relevant information will aid police in the investigation of a future or past offence.[87] The latter standard is higher than the reasonable suspicion standard for obtaining an IP address. As

---

81 See *Bykovets*, *supra* note 2 at para 85.

82 See *Criminal Code*, *supra* note 9, s 487.015(1).

83 *Ibid*, s 487.015(2).

84 See *R v Chehil*, 2013 SCC 49 at para 27 [*Chehil*].

85 See e.g. *Spencer*, *supra* note 4 (the undercover officer traded child sex abuse materials via email with the offender which resulted in the offender's IP address being disclosed).

86 See *Criminal Code*, *supra* note 9, s 487.014(1).

87 *Ibid*, s 487.014(2).

the Supreme Court explains, "while reasonable grounds to suspect and reasonable … grounds to believe are similar in that they both must be grounded in objective facts, reasonable suspicion is a lower standard, as it engages the reasonable possibility, rather than probability, of crime."[88]

It is unlikely that separate applications will be required in every instance, though the nuances of online crime investigations may render this necessary in some circumstances. As Justice Karakatsanis observes in *Bykovets*, "[w]here the IP address, or the subscriber information, is sufficiently linked to the commission of a crime, judicial authorization is readily available and adds little to the information police must already provide for a *Spencer* production order."[89] Thus, it is entirely possible—and would add minimal additional strain on police resources—to combine a *Spencer* application with a *Bykovets* application.[90] Requiring such an application nevertheless raises the question: does the reasonableness branch of section 8 of the *Charter* require a court order to make requests for IP addresses and subscriber information in all contexts? This is not clear from *Spencer* or *Bykovets* because neither decision concluded anything other than the search was unreasonable because it was not "authorized by law."

B) Administrative Demand

All of the justices in *Bykovets* were deeply concerned about how certain online crime threatens vulnerable parties like children.[91] Similar concerns were also voiced by the Supreme Court in *Spencer*[92] and by commentators expressing angst towards the implications of the latter decision for effectively investigating these crimes.[93] Detective Sergeant Kim Gross was particularly outspoken post-*Spencer*. As she observed:

> [T]he paperwork involved with obtaining a [production order] is extensive. Depending on the circumstances, it could take an officer days or even weeks to construct a [production order]. At that point we must wait for approval from a Justice of the Peace … and then submit it to the ISP to be fulfilled. At the point it

---

88 See *Chehil*, *supra* note 84 at para 27.

89 See *Bykovets*, *supra* note 2 at para 85.

90 It is notable that my acknowledgment that the likely "minimal" intrusion inherent to combining these applications does not mean that I agree with Justice Karakatsanis that this justifies reliance on a reasonable hypothetical. See the argument in Part I, *above*.

91 See *Bykovets*, *supra* note 2 at paras 84, 139, 156–60.

92 See *Spencer*, *supra* note 4 at para 80.

93 See Patricia Joseph, "A TheCourt.ca Exclusive Interview: R v Spencer One Year Later" (24 September 2015), online: <tinyurl.com/2s9595zh> [perma.cc/AWT4-MGXU].

> reaches the ISP, it often takes 30 days to receive the subscriber information back from the company.[94]

The efficiency concerns inherent to the production order process—which would be aggravated to some extent if a transmission data order were required in addition to a production order—are therefore of concern as they slow down police investigations. In some cases, police raise concerns over whether these additional burdens will limit their ability to thoroughly pursue an investigation or have time to investigate other leads.[95] It is therefore unsurprising that police describe the long-term consequences of *Spencer* (and presumably *Bykovets*) as "extremely detrimental."[96]

Given these concerns, Parliament may wish to craft more permissive transmission data/production order laws targeting crimes like possession and distribution of child sex abuse materials and child luring offences.[97] In so doing, however, Parliament will face obstacles given the comments from the majority in *Bykovets* about the minimal impact applying for a court order imposes on law enforcement. But those comments did not take into account the pitfalls already in place for investigating online crimes identified by police following *Spencer*. Instead, the Court in *Bykovets* appears to assume that a production order is constitutionally required before subscriber information may be compelled from an ISP. If true, then the additional limitations imposed by *Bykovets* indeed seem minimal. However, the Court in *Spencer* only concluded that the search was unreasonable because it was not "authorized by law." It said nothing about what requirements would render an authorizing law reasonable. The production order—a general police power—was simply not crafted with the *Spencer* circumstance in mind.

The majority in *Bykovets* accordingly overlooks the actual law enforcement concerns arising from requiring police to apply to a court to compel production of IP addresses and ISP subscriber information. The issue is not with making out evidentiary grounds to support such a search, as Justice Karakatsanis suggests. Indeed, the state will have little difficulty proving the requisite grounds to satisfy these orders given the nature of many investigations. This is true in fact scenarios like *Bykovets* where a clearly fraudulent transaction occurred. However, I would not go so far as to conclude that this will be true when investigating all fraud crimes. This suggests that some additional caution may be warranted given the nature of

---

94 *Ibid.*

95 *Ibid.*

96 *Ibid.*

97 See *Bykovets*, *supra* note 2 ("the case law is replete with examples of police investigating offences against children, including child [sex abuse material] and child luring, using IP addresses" at para 159).

such crimes. In typical child sex abuse material investigations,[98] however, undercover police officers engage in conversations with pedophiles online and trade materials with them. Upon so doing, police receive all the information needed to know that a crime was committed.[99] The only issue is *who* committed the crime. The IP address typically received as a result of engaging in online communications and the subsequent subscriber information from the ISP provide an answer to that question.

It is nevertheless notable that it is no longer clear whether even the *Spencer* procedure is constitutional after *Bykovets*. Must police now apply for a court order to use the IP address to reveal the ISP—a step necessarily preceding any application for a production order to reveal subscriber information? After all, police *could* use the IP address at this stage in other ways to reveal internet conduct. Applying the majority's rationale in *Bykovets*, any seizure of an IP address—even to reveal the ISP—should violate section 8 of the *Charter*. It is arguable that such a practice will not give rise to a violation of section 8 of the *Charter* as the plain view and/or abandonment doctrines may allow police to use the IP address in this limited manner.[100] However, that issue is likely to be litigious following *Bykovets*. As opposed to requiring courts to resolve this complex question, I take the view that it would be preferable for Parliament to pass a law permitting police to access IP addresses and ISP subscriber information upon administrative demand.

To determine whether such a law would be constitutional, it is necessary to unpack the state interests inherent to investigations implicating child sex abuse material. Three points are clear from the preceding discussion: (i) the Supreme Court justices in *Spencer* and *Bykovets* all share the view that sexual offences against children are insidious;[101] (ii) fighting online crime is particularly difficult given the inherently anonymous nature of the internet; and (iii) pursuant to common investigative methods like that at issue in *Spencer* it will be clear that a serious offence like possession or distribution of child sex abuse material—very much a "know it when you see it" type of offence—was committed by whoever was using the IP

---

98 I recognize that not all investigations unfold in this manner. In cases where police come by information via a witness, though, police will typically know the name of that person and could apply for a warrant to seize and search the relevant computer. My comments here are meant to be limited to the types of fact patterns that arise in cases like *Spencer*, *supra* note 4, which are "common" as I explain below.

99 See Fehr, "Administrative Demand", *supra* note 16.

100 See e.g. *Patrick*, *supra* note 44 at para 20 (describing the abandonment doctrine); *R v McGregor*, 2023 SCC 4 at paras 37–38 (describing the plain view doctrine).

101 See *Spencer*, *supra* note 4 at para 80; *Bykovets*, *supra* note 2 at paras 84, 139, 156–60.

address received during the police investigation.[102] The pressing nature of these offences all make it reasonable to ask: can a law be developed to help police work more efficiently in contexts where serious offences are committed, and police have a clear pathway to prove who committed the offence? In particular, should not the police be able to make an administrative demand per an authorized law for IP addresses and/or ISP subscriber information to receive this information?

While I have made such a proposal before,[103] it is prudent to restate and build upon that argument post-*Bykovets*. In so doing, it is important to recognize and give substantial weight to the important privacy concerns at stake when the state accesses both an IP address and ISP subscriber information. For such a law to survive constitutional scrutiny, it is therefore important to put in place substantial restrictions that serve to protect these important privacy interests.[104] First, as alluded to earlier, the type of investigation for which an administrative demand might survive constitutional scrutiny must be limited to serious offences that are otherwise difficult to investigate and involve a means of investigation that involves the state receiving clear evidence that a crime was committed. The factual scenario in *Spencer* is common and illustrative. The offender traded child sex abuse materials with an undercover officer. Upon receiving the material from the offender, the officer knew the individual's IP address, and there was no reasonable doubt that the possession and distribution offences were committed.[105]

Second, the administrative demand law that I am proposing would put in place safeguards to ensure broad access to a user's internet history is not permissible. If an IP address is retrieved, the law could readily be tailored to prohibit use of the IP address to uncover any internet activity in the ways identified by the Supreme Court in *Bykovets*.[106] This should not pose a significant concern for law enforcement as they typically do not want the information for that purpose. While the majority in *Bykovets* correctly observed that an IP address *could* be so used, the investigating officers in that case explicitly stated that they had no such intention as such a search was unnecessary to forward their investigation. This followed because they could learn the identity of the accused much more readily by applying for a production order under section 487.014 of the *Criminal Code* requiring the ISP to disclose the relevant subscriber information.

---

102 See e.g. Andrea Slane, "Privacy and Civic Duty in *R v Ward*: The Right to Online Anonymity and the *Charter*-Compliant Scope of Voluntary Cooperation with Police Requests" (2013) 39:1 Queen's LJ 301 at 303.

103 See Fehr, "Administrative Demand", *supra* note 16.

104 *Ibid.*

105 See *Spencer*, *supra* note 4 at para 7.

106 See *Bykovets*, *supra* note 2 at paras 60–70.

State access to ISP subscriber information raises different issues. This information inherently reveals the identity of the accused and attaches the accused to particular internet activity. It does not follow, however, that the state gains access to the offender's entire internet history. Unfortunately, this issue was not resolved by the Supreme Court in *Spencer* because there was "little information in the record about the nature of IP addresses in general or the IP addresses provided by [the ISP] to its subscribers."[107] In *R v Ward*,[108] however, Justice Doherty observed that the investigating officers had access to only seconds of the user's internet activity.[109] As such, he concluded that "what is revealed is more in the nature of a snapshot than a history of one's Internet activity."[110] To obtain a broader internet history, the state needed to conduct a *further* search to match the IP address to other internet activity associated with that IP address.[111] As the Office of the Privacy Commissioner observes,[112] such a search may be completed with tools such as WHOIS, an "online service used for … querying databases that store the registered users or assignees of domain names or IP address blocks."[113] These searches should also be subject to a warrant requirement. In the common child sex abuse material investigation, however, police have all the information relevant to pursuing their investigation after securing the ISP subscriber information. With this information, they can secure a warrant to search the accused's residence to retrieve and search their computer where the actual incriminating evidence will be located.

Third, and related to the latter point, legitimate concerns may arise over whether the state would abuse access to IP addresses and subscriber information. While police urged the public to trust them with this information post-*Spencer*,[114] it is important to recognize that the number of yearly requests for ISP subscriber information in Canada pre-*Spencer* greatly outnumbered prosecutions for online crimes.[115] I agree with Matthew Ponsford that it is therefore "reasonable to infer that police were at times making requests which were more akin to fishing expeditions than

---

107 See *Spencer*, *supra* note 4 at para 8.

108 2012 ONCA 660 [*Ward*].

109 *Ibid* at para 25.

110 *Ibid*. See also para 18.

111 See Fehr, "Administrative Demand", *supra* note 16.

112 See Office of the Privacy Commissioner of Canada, "What an IP Address Can Reveal About You" (May 2013) at 2–7, online (report): <tinyurl.com/52v29n2s> [perma.cc/Y4A9-HNWG].

113 *Ibid* at 2.

114 See Joseph, *supra* note 93.

115 See generally Matthew Ponsford, "The Lawful Access Fallacy: Voluntary Warrantless Disclosures, Customer Privacy, and Government Requests for Subscriber Information" (2017) 15:1 CJLT 153.

searches founded upon a reasonable basis."[116] But this possibility can again be adequately monitored by requiring that police report both the number of searches undertaken for the narrow crimes for which the proposed search power would be permissible and the corresponding number of criminal charges. A requirement that the police delete data with respect to any information received that did not lead to a criminal charge could also be enacted to better protect privacy interests. Notably, similar limitations were constitutionally required for warrantless interception orders permitted under Part VI of the *Criminal Code*.[117]

Finally, it would be desirable to provide a more drastic remedy in the case of state abuse of informational privacy in the context of criminal investigations. In particular, a rule requiring automatic exclusion of any evidence obtained as a result of improper use of an IP address or ISP subscriber information would be prudent. Thus, if the police used an IP address to reveal the identity of the user or employed online databases to reveal more than a "snapshot" of internet activity as a result of receiving ISP subscriber information associated with an IP address under investigation, all the incriminating information received from these searches would be inadmissible. In my view, such a rule would provide a strong deterrent for police and would adequately encourage them to seek lawful process if they wished to conduct broader searches. Such an approach would also prevent the circumstance from arising where the accused must launch a broad constitutional challenge to vindicate their rights. After establishing the breach factually, the remedy would simply flow from the statute.

Conclusion

The Supreme Court's decision in *Bykovets* to recognize a reasonable expectation of privacy in an IP address is principled in the abstract given that such access may reveal online activity. However, the majority's choice to find a reasonable expectation of privacy relying upon a hypothetical scenario was inadequately defended. While the additional restraints on law enforcement imposed by the majority are minimal, the fact that no privacy interests were breached in *Bykovets* makes even a minimal intrusion onto law enforcement interests difficult to accept. Legal process considerations and the counter-majoritarian role of courts nevertheless militate in favour of allowing judges to utilize hypothetical scenarios to recognize a reasonable expectation of privacy in some circumstances. This is especially prudent in the digital privacy context given the difficulties accused encounter when attempting to prove such violations. As the

---

116 See Fehr, "Administrative Demand", *supra* note 16, citing Ponsford, *supra* note 115.

117 See *R v Tse*, 2012 SCC 16.

Court explained when justifying the use of hypothetical scenarios in the context of section 12 of the *Charter*, such an approach can help ensure that "bad laws" are inoperative. Similarly, use of hypothetical scenarios in the section 8 context can help ensure that "bad investigative practices" are adequately deterred.

Such an approach is also prudent as it encourages Parliament to legislate criminal procedure rules in an area where its legislation is woefully underdeveloped.[118] More specifically, Parliament may rely upon law enforcement interests to justify passing a law permitting the state to demand IP addresses and ISP subscriber information in relation to limited investigations. The most obvious candidates for such a police power relate to possession and distribution of child sex abuse materials. The insidious nature of these offences when combined with the difficulties police face investigating them and the fact that police will know during a typical investigation that the individual behind the IP address committed an offence makes it an ideal candidate for my proposed police power. In addition, the need for police to utilize scarce resources efficiently—and the reality that making court applications places significant demands on finite police resources—militates in favour of such laws provided there are sufficient privacy protections in place. In addition to the limited offences to which such a power should apply, privacy protections could be enacted to restrict how police make use of the information received and seek to maximally deter police misuse of any data. The latter aim could be furthered by providing a broad exclusionary remedy that would effectively forestall the initial investigation if any misuse of an IP address or ISP subscriber information were uncovered.

---

118 For a detailed review, see Fehr, "Institutional Approach", *supra* note 13.